An approach for using biometrics and cryptography for E-Authentication

James MacLean
3M
jemaclean@mmm.com
613-722-2070

Issues with Open Networks

- PC's and the internet are inherently an untrustworthy environments
- Numerous access points
- Clients may move from one PC to another, depending on time of day or service they are accessing.
- Most clients will be trustworthy, but need to be audited at all access points
- Malicious clients will attempt to extend their entitlement by sharing or copying passwords or cracking tokens

Privacy Issues

- Identity theft is a growing problem.
- Eavesdropping may allow skim information that can be used to social engineering
- The use of personal information for more than it was initially intended.

Approaches to Authentication

- **Levels 3 and 4 require high confidences in the asserted identity**
  - **Hardware token combining biometrics and cryptography is need.**
  - **Soft cryptographic tokens are open to prolonged repeated attacks.**
  - **Passwords don’t provide a high enough level of none repudiation.**

Requirements of biometric token

- private key carrier
- protected by biometric
- cryptographic processor
- generation of keys on token
- Biometric match on token
- personal token.

Strongly Authenticates Users

- cryptographic private key confirms identity of unit
  - public key stored on the network Credential Service Provider (CSP)
  - The verifier and token mutually authenticate via challenge / response
- biometric ties unit to registered user
  - fingerprint “unlocks” private key
  - unit does not function without registered user
- protects individual privacy
  - fingerprint never leaves personal device
  - each device unique to an individual

Enhances Security & Privacy

- Digital signatures at the touch of a finger
  - Specific transactions can be signed at the same time as they are created
- Personal identifying information does not need to be stored on the token.
  - The verify provides the minimal level of identification information required by the relying party.
  - Supports both anonymous and strongly authenticated transaction.

3M™ VeriMe™ Personal Biometric Authenticator

- private key carrier
- protected by biometric
- cryptographic processor
- private key, biometric template never leave the device
- wearable, personal

3M™ VeriMe™ Personal Biometric Authenticator

- security
  - strong authentication via biometrics, cryptography
- privacy
  - access policy, auto logoff, observer detection
  - Wireless communications
- productivity
  - simplified logon, single sign-on, digital signing